CLAIMS

What is claimed is:

1. An authentication method comprising:

generating an initialization vector at a first electronic device;

determining at the first electronic device whether the initialization vector falls within a first group of initialization vectors, the first group includes a plurality of initialization vectors solely used in connection with an authentication sequence; and

encrypting information using in part the initialization vector for return to a second electronic device if the initialization vector falls within the first group.

2. The authentication method of claim 1, wherein the first electronic device is a wireless unit.

3. The authentication method of claim 1, wherein the second electronic device is an access point.

4. The authentication method of claim 1, wherein prior to generating the initialization vector, the method comprises receiving the information from the second electronic device by the first electronic device.

5. The authentication method of claim 4, wherein the information is a challenge text.

6. The authentication method of claim 5, wherein the challenge text is a first sequence of bits and the initialization vector is a second sequence of bits produced by a number generator.

7. The authentication method of claim 4, wherein the number generator is a pseudo-random number generator.

8. The authentication method of claim 1 further comprising regenerating an initialization vector if the initialization vector fails to fall within the first group.

9. The authentication method of claim 1, wherein the determining whether the initialization vector falls within the first group includes determining whether a selected series of bits of the initialization vector has been set.

10. The authentication method of claim 9, wherein the selected series of bits is continuous.

11. The authentication method of claim 5, wherein prior to receiving the challenge text, the method further comprises negotiating a shared secret key between the first electronic device and the second electronic device.

12. The authentication method of claim 11, wherein the encrypting of the information includes

combining the initialization vector with the shared secret key; and

repeatedly performing bitwise Exclusive-OR (XOR) operations on the challenge text using a combination of the initialization vector with the shared secret key.

13. The authentication method of claim 5 further comprising:

transmitting both the encrypted challenge text and the initialization vector to the second electronic device;

decrypting the encrypted challenge text using both the initialization vector and a prestored copy of the shared secret key to recover a challenge text; and

comparing the recovered challenge text with the challenge text.

14. A method for authenticating a wireless unit in communications with an access point, comprising:

transmitting a challenge text from the access point to the wireless unit;

receiving an encrypted challenge text and an initialization vector from the wireless unit;

decrypting the encrypted challenge text using both the initialization vector and a pre-stored copy of a shared secret key to recover a challenge text; and

comparing the recovered challenge text with the challenge text previously transmitted to the wireless unit.

15. The method of claim 14, wherein the challenge text is a first sequence of bits.

16. The method of claim 15, wherein the initialization vector is a second sequence of bits produced by a number generator.

17. The method of claim 16, wherein the number generator is a pseudo-random number generator.

18. The method of claim 14, wherein prior to transmitting the challenge text, the method further comprises negotiating the shared secret key between the access point and the wireless unit.

19. The method of claim 14, wherein the decrypting of the encrypted challenge text includes

combining the initialization vector with the shared secret key; and

using a combination of the initialization vector and the shared secret key as a key material loaded to decrypt the encrypted challenge text.

20. A method comprising:

selecting a bit size (N) of an initialization vector;

partitioning all 2^N initialization vectors into a first group and a second group;

using an initialization vector from the first group exclusively for authentication; and

using an initialization vector from the second group exclusively for data communications.

21. The method of claim 20, wherein the authentication is Wired Equivalent Privacy (WEP) authentication in accordance with Institute of Electrical and Electronics Engineers (IEEE) 802.11.

22. The method of claim 20, wherein a first predetermined number of initialization vectors associated with the first group is substantially less than a second predetermined number of initialization vectors associated with the second group.

23. The method of claim 20, wherein the data communications include wired equivalent privacy (WEP) encryption and WEP decryption operations.

24. An electronic device comprising:

a memory to contain a plurality of keys including a shared secret key;

a number generator;

a device management logic in communication with the memory and the number generator, the device management logic including

logic configured to analyze an initialization vector generated from the number generator to determine whether the initialization vector is used for either wired authentication or data communications; and

a wireless transceiver to transmit and receive information for configured to support the authentication.

25. The electronic device of claim 24, wherein the authentication is Wired Equivalent Privacy (WEP) authentication.

26. The electronic device of claim 24 is an access point.

27. An electronic device comprising:

means for generating an initialization vector;

means for determining whether the initialization vector falls within a first group of initialization vectors, the first group includes a plurality of initialization vectors solely used in connection with an authentication sequence; and

means for encrypting information using the initialization vector for return to a source for the information using in part the initialization vector if the initialization vector falls within the first group.

28. A software module implemented for execution by an electronic device, the software module comprising:

a first module to select a bit size (N) of an initialization vector;

a second module to partition all 2^N initialization vectors into a first group and a second group;

a third module to use an initialization vector from the first group exclusively for authentication; and

a fourth module to use an initialization vector from the second group exclusively for data communications.